National Defence / Défense nationale

L'APPLICATION DES CODES DE COSTAS ET DES CODES À CONGRUENCES QUADRATIQUES À LA COMPRESSION D'IMPULSION NUMÉRIQUE

par

C. Delisle et M. Blanchette
Section du radar de surface
Division du radar

CENTRE DE RECHERCHES POUR LA DÉFENSE, OTTAWA
NOTE TECHNIQUE No. 91-31

PCN
041LC

Décembre 1991
Ottawa

RÉSUMÉ

Ce document étudie l'application à la compression d'impulsion numérique de deux types de codage de la fréquence: les codes de Costas et les codes à congruences quadratiques. Ces codes ont la particularité de produire des diagrammes d'ambiguïté en forme de punaise avec de faibles lobes secondaires. Ce rapport traite des différents algorithmes de construction, de l'évaluation des fonctions d'auto-corrélation et de corrélation croisée, et de leur comparaison à des codes connus. Bien qu'ayant des résultats intéressants pour le nombre de codes disponibles et le niveau des lobes secondaires, ils semblent être moins performants sur ces points que les codes pseudo-aléatoires, "chirp" et "step-chirp".

ABSTRACT

In this report we present the analysis and construction methods for two types of frequency coded pulses: (a) Costas codes and (b) quadratic congruential codes. These codes have the characteristic of producing a thumbtack ambiguity diagram with low sidelobes. Computer simulations were performed to calculate their autocorrelation functions. Comparative evaluation of the performance of these codes and well known codes was carried out. Results showed that Costas codes and quadratic congruential codes have low sidelobes but not as low as the chirp, step-chirp or pseudo-random codes.

EXECUTIVE SUMMARY

La compression d'impulsion numérique peut être utilisée dans un radar à fonctions multiples comme contre-contre-mesure électronique pour contrer le brouillage. La sélection aléatoire d'un nouveau code à chaque transmission permet de détecter les retours possédant le même code que celui de l'impulsion transmise tout en rejetant les retours ayant tout autre code. Il est important de choisir les codes pour que leur fonction d'auto-corrélation ait un lobe principal étroit et des lobes secondaires très faibles, et que leur corrélation croisée soit beaucoup plus faible que leur auto-corrélation respective.

Ce document étudie l'application à la compression d'impulsion numérique de deux types de codage de la fréquence; les codes de Costas et les codes à congruences quadratiques. Ces codes ont la particularité de produire des diagrammes d'ambiguïté en forme de punaise tout en ayant de faibles lobes secondaires. Ce rapport traite des différentes méthodes de construction, de l'évaluation sur ordinateur des fonctions d'auto-corrélation et de corrélation croisée, et de leur comparaison à des codes connus, tels les codes biphases pseudo-aléatoires et les codes modulés en fréquence chirp et step-chirp.

Les fonctions d'auto-corrélation et de corrélation croisée ont été examinées pour des codes de longueur voisine de 128, limite fixée par l'appareillage déjà existant et utilisée lors de précédentes recherches sur d'autres codes. Suite à l'analyse des résultats, les codes de Costas ont été trouvés les meilleurs en ce qui concerne la fonction d'auto-corrélation, surtout avec la méthode de construction de Welch, alors que les codes quadratiques offrent de meilleurs résultats pour la corrélation croisée. Cependant, les fonctions d'auto-corrélation de ces codes possèdent des lobes secondaires plus élevés que celles des codes chirp, step-chirp et pseudo-aléatoires équivalents.

Les codes de Costas et les codes quadratiques peuvent être utilisés pour la compression d'impulsion numérique mais ne sont pas aussi performants que les codes pseudo-aléatoires, chirp et step-chirp en ce qui a rapport au niveau des lobes secondaires des fonctions d'auto-corrélation et au nombre de codes disponibles. Les codes quadratiques sont plus appropriés pour une utilisation nécessitant un compromis entre une bonne fonction d'auto-corrélation et une bonne corrélation croisée.

92-03932/

TABLE DES MATIÈRES

RÉSUMÉ iii

ABSTRACT iii

EXECUTIVE SUMMARY v

TABLE DES MATIÈRES vii

1. INTRODUCTION 1

2. LES CODES DE COSTAS 3
   2.1 MÉTHODE DE WELCH 6
   2.2 MÉTHODE DE GOLOMB 9

3. LES CODES À CONGRUENCES QUADRATIQUES 12

4. COMPARAISON DES DIFFÉRENTS TYPES DE CODES 15

5. CONCLUSION 19

BIBLIOGRAPHIE BIB-1

1. INTRODUCTION

Les signaux codés sont utilisés pour les radars à compression d'impulsion. Ils permettent d'améliorer la résolution et la détection des cibles sans à avoir augmenter la puissance crête émise. Les impulsions transmises sont modulées en fréquence ou en phase selon un code spécifique. À leur retour, les impulsions sont traitées avec un filtre adapté au code utilisé lors de la transmission. La sortie du filtre représente la fonction de corrélation entre l'impulsion transmise et l'impulsion reçue. Pour pouvoir détecter des signaux faibles proches de signaux plus forts, la fonction d'auto-corrélation du code devrait idéalement comporter un pic principal élevé et étroit, et des pics secondaires faibles et tous de même amplitude. En pratique, on obtient souvent des pics secondaires élevés que l'on doit chercher à minimiser.

Dans certaines applications, le radar utilise l'agilité de codage qui consiste à utiliser un code différent à chaque transmission. Cette technique de contre-contre-mesure électronique permet de détecter les cibles possédant le même code que celui de l'impulsion transmise, et de rejeter le brouillage et les échos lointains dont les cibles ont un code différent. Il est alors nécessaire que la corrélation croisée entre les codes successifs ne comporte que des pics faibles.

La corrélation croisée pourra admettre des pics dominants à condition qu'ils soient décentrés pour ne pas ressembler à une auto-corrélation. D'une impulsion à l'autre, les pics principaux des cibles renvoyant le bon code sont toujours au même endroit, tandis que les pics dominants des cibles possédant un code différent sont détectées à des positions diverses. La détection cumulative ou l'intégration cohérente permet de concentrer la détection des retours avec le bon code, tout en éparpillant les détections des retours dont le code ne correspond pas à celui transmis [1,2,3].

Il existe différentes méthodes de codage de signaux. Une modulation discrète de la fréquence peut être obtenue en échantillonnant une modulation continue de la fréquence. Également, l'échantillonnage de la phase d'un signal modulé en fréquence peut être utilisé pour un codage de la phase. Nous étudierons quelques types de codage en fréquence suggérés pour la compression d'impulsion tels que les codes de Costas [4,5,6,7] et les codes à congruences quadratiques [8,9,10] et les comparerons à d'autres codes déjà utilisés en radar comme les codes chirp, step-chirp et pseudo-aléatoires [11,12,1]. Tous les codes étudiés ont une longueur voisine de 128 car l'appareillage disponible, construit lors d'études précédentes sur d'autres codes, peut produire des codes ayant au maximum 128 points [12,13].

Pour étudier les propriétés des codes et déterminer quel type donne les meilleures fonctions d'auto-corrélation et de corrélation croisée, nous avons construit un logiciel qui simule la corrélation entre les signaux transmis et reçu. En premier, un algorithme différent pour chaque code est utilisé pour calculer la fréquence et la phase instantanées du signal désiré. Par la suite, le programme simule l'échantillonnage des composantes en phase et en quadrature (I & Q) d'un signal en produisant une séquence de variables complexes. Finalement, des transformées de Fourier rapide sont employées pour effectuer la corrélation entre les séquences transmise et reçue. Le logiciel calcule également la valeur du pic central, du pic secondaire maximum et la moyenne des pics secondaires de la corrélation. Pour chaque fonction d'auto-corrélation des codes étudiés, la largeur et la hauteur du pic principal sont toujours respectivement égales à un et à la longueur du code.

2. LES CODES DE COSTAS

Les codes étudiés dans ce rapport s'appliquent à une modulation discrète de la fréquence. Les impulsions sont divisées en segments et la fréquence du signal varie avec chacun des segments. Une matrice est utilisée pour représenter le codage en fréquence d'un signal. Si a(n) représente la position de l'élément dans la matrice du code, la fréquence de chaque segment est donnée par:

$$f(n) = f_o + a(n) \cdot B/N \qquad (1)$$

où f_o est la fréquence initiale du signal, B la largueur de bande du signal, et N le nombre de segments.

Un code de Costas est une matrice représentant la fréquence en fonction du temps pour le signal codé. La matrice comme celle de la figure 1 ne possède qu'une seule fréquence pour chaque intervalle de temps et un seul intervalle de temps pour chaque fréquence. Il y a N éléments présents dans une matrice d'un code de Costas et la position de ces éléments est une permutation de l'ensemble {1,2,...,N}.

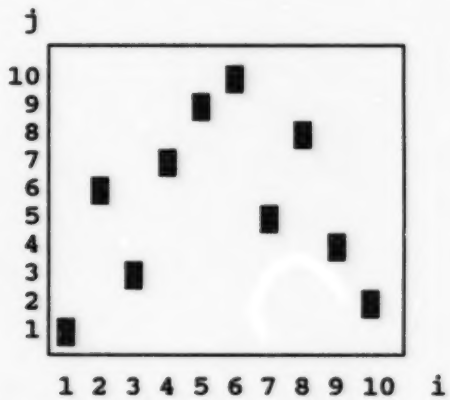


Figure 1 Code de Costas (méthode de Welch; q=11,α=6,η=2).

Un code répond au critère de Costas si, en superposant la matrice et une version décalée d'elle-même, au plus deux éléments coïncident, et ce pour n'importe quel décalage non nul en temps et/ou en fréquence. Le critère de Costas permet aux codes de Welch et de Golomb, ainsi qu'aux autres codes de Costas, d'avoir un diagramme d'ambiguïté et une fonction d'auto-corrélation quasi-idéaux, c'est-à-dire une pointe centrale et des lobes secondaires d'amplitude faible et constante sur toute la région.

Les constructions de codes de Costas étudiées sont basées sur la théorie des corps de Galois [14]. Un corps de Galois est un

ensemble dont la dimension (q) est un nombre premier tel qu'il existe l'ensemble GF(q) = {0,1,2,...,q-1} sur lequel les opérations arithmétiques se font modulo q. Un élément primitif d'un corps de Galois permet d'exprimer tous les éléments non nuls de l'ensemble par une puissance de ce nombre(modulo q). Chaque ensemble fini possède plusieurs éléments primitifs. Soit un corps de Galois GF(q) où q, la dimension de l'ensemble, est un nombre premier. On peut décomposer le nombre q-1 par une factorisation de nombre premier:

$$(q-1) = p_1^{m1} \cdot p_2^{m2} \cdot \ldots \cdot p_r^{mr} \qquad (2)$$

Le nombre d'éléments primitifs de l'ensemble GF(q) est alors donné par :

$$\phi(q-1) = p_1^{m1-1} \cdot p_2^{m2-1} \cdot \ldots \cdot p_r^{mr-1} \cdot (p_1 - 1) \cdot \ldots \cdot (p_r - 1) \qquad (3)$$

Par exemple, pour un ensemble GF(11), le corps de Galois servant à générer le code est l'ensemble suivant:

$$GF(11) = \{0,1,2,3,\ldots,10\}$$

Dans ce cas-ci, q=11; on peut donc exprimer par factorisation

$$(q-1) = 10 = 2^1 \cdot 5^1$$

Le nombre d'éléments primitifs de ce corps de Galois se calcule comme suit d'après l'équation (3):

$$\phi(q-1) = \phi(10) = 2^0 \cdot 5^0 \cdot (1) \cdot (4) = 4$$

L'ensemble GF(11) possède donc quatre éléments primitifs. Le nombre six est un des éléments primitifs de GF(11) car les puissances de ce nombre, modulo 11, redonnent tous les éléments non nuls de l'ensemble GF(11) = {0,1,2,...,10}.

$$\begin{aligned} 6^1 &= 6 \\ 6^2 &= 3 \\ 6^3 &= 7 \\ 6^4 &= 9 \\ 6^5 &= 10 \\ 6^6 &= 5 \\ 6^7 &= 8 \\ 6^8 &= 4 \\ 6^9 &= 2 \\ 6^{10} &= 1 \end{aligned}$$

Prenons un élément primitif α d'un corps de Galois GF(q). On remarque que

$$\alpha^{q-1}\big|_{\text{mod } q} = 1$$

et que pour n'importe quel entier i,

$$\alpha^i\big|_{\text{mod } q} = (\alpha^{i-1}\big|_{\text{mod } q} \cdot \alpha)\big|_{\text{mod } q}$$

ce qui permet de calculer les puissances d'un élément primitif par récursivité [15]. Cette méthode présente l'avantage de toujours traiter des nombres plus petits que α^2.

La liste des éléments primitifs des corps de Galois utilisés dans ce texte est donnée dans le tableau 1.

GF(q)	Éléments primitifs
11	2, 6, 7, 8
17	3, 5, 6, 7, 10, 11, 12, 14
19	2, 3, 10, 13, 14, 15
101	2, 3, 7, 8, 11, 12, 15, 18, 26, 27, 28, 29, 34, 35, 38, 40, 42, 46, 48, 50, 51, 53, 55, 59, 61, 63, 66, 67, 72, 73, 74, 75, 83, 86, 89, 90, 93, 94, 98, 99
127	3, 6, 7, 12, 14, 23, 29, 39, 43, 45, 46, 48, 53, 55, 56, 57, 58, 65, 67, 78, 83, 85, 86, 91, 92, 93, 96, 97, 101,106, 109, 110, 112, 114, 116, 118
131	2, 6, 8, 10, 14, 17, 22, 23, 26, 29, 30, 31, 37, 40, 50, 54, 56, 57, 66, 67, 72, 76, 82, 83, 85, 87, 88, 90, 93, 95, 96, 97, 98, 103, 104, 106, 110, 111, 115, 116, 118, 119, 120, 122, 124, 126, 127, 128

Tableau 1 Éléments primitifs de certains corps de Galois.

Différents types de constructions permettent d'obtenir des codes répondant au critère de Costas. Nous étudierons les méthodes de Welch et de Golomb. Ces codes de Costas sont générés à partir d'un corps de Galois GF(q) où (q-1) et (q-2) représentent respectivement le nombre d'éléments pour les codes de Welch et de Golomb.

2.1 MÉTHODE DE WELCH

D'après Welch, on obtient un code de Costas si α est un élément primitif de GF(q), η est un élément non nul de l'ensemble et q est un nombre impair et premier. La matrice du code se construit comme suit:

$$(i,j) = (i, \eta \cdot \alpha^i \big|_{\text{mod } q}) \qquad (4)$$

i : position horizontale
j : position verticale
$1 \leq i,j \leq q-1$

Cette méthode produit $(q-1)\cdot\phi(q-1)$ codes différents de dimension $(q-1)\cdot(q-1)$. C'est-à-dire que l'on peut générer (q-1) codes avec le même élément primitif en variant la valeur du coefficient η. Ces différents codes générés par le même élément primitif ne sont, en fait, que des rotations cycliques l'un de l'autre.

Pour illustrer un code de Welch, prenons le corps de Galois GF(11). La longueur du code généré sera de 10. En choisissant 6 comme élément primitif et un coefficient égal à 2, nous obtenons la matrice de la figure 1, où les valeurs de i et j sont:

i	$j = 2\cdot 6^i \big\|_{\text{mod } 11}$
1	$2\cdot 6^1 = 1$
2	$2\cdot 6^2 = 6$
3	$2\cdot 6^3 = 3$
4	$2\cdot 6^4 = 7$
5	$2\cdot 6^5 = 9$
6	$2\cdot 6^6 = 10$
7	$2\cdot 6^7 = 5$
8	$2\cdot 6^8 = 8$
9	$2\cdot 6^9 = 4$
10	$2\cdot 6^{10} = 2$

Prenons un code de Welch de longueur 126 ayant un produit temps-largeur de bande (BT) de 126, 126 éléments, le nombre 6 comme élément primitif et un coefficient de 22. Pour ce code, nous obtenons des pics secondaires de l'auto-corrélation à -24.0 dB par rapport au pic central. Changeons cette fois pour un élément de 116 et un coefficient de 111, nous obtenons alors un pic secondaire maximal de -20.3 dB sous la valeur du pic principal.

Il y a au total 4536 (36·126) possibilités de codes de Welch possédant 126 éléments. Pour chacune de ces possibilités, le pic secondaire maximum se situe entre -20.3 dB et -24.0 dB du pic central. Le graphique de la figure 2 représente la fonction d'auto-corrélation d'un code de Welch dont les paramètres longueur,

produit BT et nombre d'éléments sont égaux à 126, l'élément primitif du code est 6 et le coefficient vaut 22.

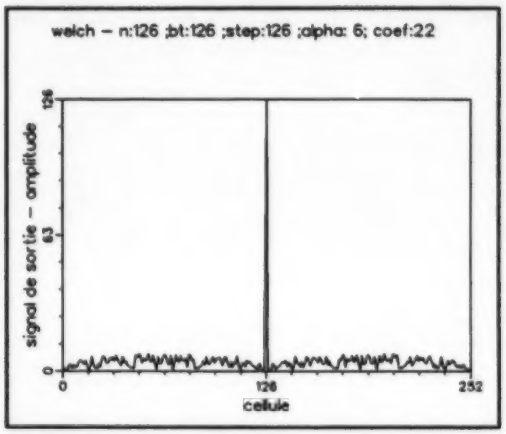


Figure 2 Auto-corrélation d'un code de Welch.

On peut avoir d'autres codes de Welch de même longueur mais avec un nombre différent d'éléments. Il s'agit d'utiliser moins d'éléments et de prendre plus d'échantillons par élément pour conserver le même nombre total d'échantillons. Cependant, la longueur du code doit être un multiple du nombre d'éléments, et le produit BT doit rester égal à la longueur du code. Nous allons étudier deux autres cas de codes de Welch.

Premièrement, un code de longueur et de produit BT de 126 avec 18 éléments fourni à partir d'un corps de Galois GF(19). Lorsque l'élément primitif est 2 et le coefficient égal à 9, le pic secondaire principal est à -18.1 dB par rapport au pic central. Pour un élément primitif de 2 et coefficient de 11, le pic est à -13.8 dB. Pour les 108 possibilités de codes de Welch de longueur et produit BT 126 possédant 18 éléments, la valeur des pics secondaires principaux se situe entre -13.8 dB et -18.1 dB sous le pic central de la fonction d'auto-corrélation.

Dans le cas de codes de longueur et produit BT égaux à 128 et un nombre d'éléments égal à 16 (fourni à partir d'un corps de Galois GF(17)), la valeur des 128 différents codes pouvant être créés varie entre -15.0 dB et -20.0 dB. Les limites sont respectivement obtenues avec des éléments primitifs de 6 et 5, et avec des coefficients de 13 et 7.

Il est aussi possible d'obtenir des codes de Costas de longueur inférieure à (q-1) à partir d'un corps de Galois GF(q) [7]. Il s'agit de retrancher des éléments de la matrice dont la valeur équivaut à un coin de la matrice. La matrice de dimension 10 correspondant au code de Welch; q=11, α=6 et η=2, et représentée

à la figure 1, peut servir d'exemple. Le premier élément de la matrice vaut 1 et le dernier vaut 2. On peut alors enlever les deux rangées et les deux colonnes contenant ces deux éléments pour obtenir un matrice de dimension 8.

Il est toujours possible d'obtenir un code de Welch de longueur (q-3) à partir du corps de Galois GF(q), si celui-ci a 2 comme élément primitif et 1 comme coefficient. Dans certains cas, elle peut être la seule possibilité. C'est ainsi que nous avons obtenu un code de Welch de longueur 128 à partir du corps de Galois GF(131).

Nous avons étudié les propriétés de ce nouveau code en calculant sa fonction d'auto-corrélation. Lorsque le produit BT est égal à la longueur du code et le nombre d'éléments, soit 128, le pic secondaire maximum est à -21.5 dB par rapport au pic central. Ces valeurs se situent dans la moyenne des résultats des codes de Welch précédemment étudiés.

Le tableau 2 contient certaines valeurs de la fonction d'auto-corrélation de différents codes de Welch étudiés .

longueur	nombre d'éléments	meilleur			pire		
		α	η	pic [dB]	α	η	pic [dB]
126	18	2	9	-18.1	2	11	-13.8
126	126	6	22	-24.0	116	111	-20.3
128	16	5	7	-20.0	6	13	-15.0
128	128	2	1	-21.5	--	--	----

Tableau 2 Auto-corrélation des codes de Welch.

Le maximum de la corrélation croisée entre deux codes de Welch a une valeur moyenne de -14 dB par rapport au pic principal de la fonction d'auto-corrélation. La corrélation croisée entre deux codes de Welch générés par le même élément primitif présente cependant un ou deux pics importants mais décentrés. Ceci est dû à la relation entre les codes ayant le même élément primitif mais non le même coefficient. Le graphique de la figure 3 présente la fonction de corrélation croisée entre deux codes de Costas générés par le même élément primitif, c'est-à-dire deux codes de Welch de longueur et produit BT de 126 et possédant 18 éléments. Les deux sont générés par un élément primitif de 2; un possède un coefficient de 9 et l'autre un coefficient de 11.

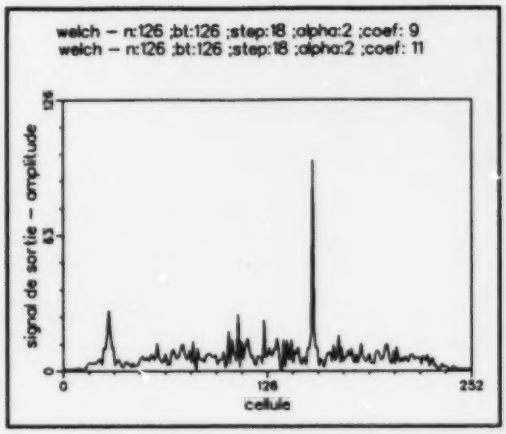


Figure 3 Corrélation croisée entre deux codes de Welch générés par le même élément primitif.

2.2 MÉTHODE DE GOLOMB

Avec la méthode de Golomb, on peut obtenir $[\phi(q-1)]^2$ codes différents de dimension $(q-2)\cdot(q-2)$. Un élément est placé dans la matrice du code en position (i,j) si et seulement si:

$$(\alpha^i + \beta^j)\Big|_{\text{mod } q} = 1 \qquad (5)$$

i : position horizontale
j : position verticale
$1 \le i,j \le q-2$

Les opérations se faisant modulo q. Les paramètres α et β sont des éléments primitifs de GF(q), q étant un nombre impair et premier.

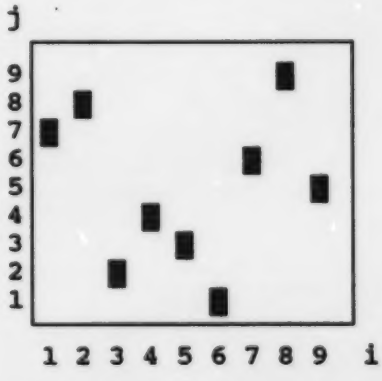


Figure 4 Code de Costas (méthode de Golomb; q=11,α=6,β=7).

Avec deux éléments primitifs du corps de Galois GF(11) tels que α=6 et β=7, on obtient un code de Golomb de longueur 9 représenté par une matrice comme celle de la figure 4, où les valeurs de i et j sont:

i	j	$(6^i + 7^j)\|_{\text{mod } 11} = 1$
1	7	$6^1 + 7^7 = 6 + 6 = 12 = 1$
2	8	$6^2 + 7^8 = 3 + 9 = 12 = 1$
3	2	$6^3 + 7^2 = 7 + 5 = 12 = 1$
4	4	$6^4 + 7^4 = 9 + 3 = 12 = 1$
5	3	$6^5 + 7^3 = 10 + 2 = 12 = 1$
6	1	$6^6 + 7^1 = 5 + 7 = 12 = 1$
7	6	$6^7 + 7^6 = 8 + 4 = 12 = 1$
8	9	$6^8 + 7^9 = 4 + 8 = 12 = 1$
9	5	$6^9 + 7^5 = 2 + 10 = 12 = 1$

La méthode de construction de Golomb génère des codes de Costas différents de ceux produits par la méthode de Welch. Prenons, par exemple, un code de Golomb fourni à partir d'un corps de Galois GF(127) où les paramètres longueur, produit BT et nombre d'éléments sont égaux à 125. Le maximum des pics secondaires des 1296 possibilités de codes varie alors entre -12.9 dB pour des éléments primitifs de 57 et 106, et de -18.6 dB pour des éléments primitifs de 7 et 55.

Le nombre d'éléments des codes de Golomb peut être différent de la longueur du code. Pour les 16 codes de Golomb de longueur et de produit BT 126 ayant 9 éléments (fourni à partir d'un corps de Galois GF(11)), le maximum des pics secondaires est de -8.9 dB sous le pic central, et ce peu importe la valeur des éléments primitifs du code. Par contre, la valeur moyenne des pics secondaires varie entre -27.5 dB et -27.8 dB respectivement pour des éléments primitifs de 6 et 6, et de 2 et 8. Les codes précédemment cités sont cependant les seules possibilités de codes de Golomb avec un nombre d'éléments non égal à la longueur du code.

Le même principe que celui utilisé pour les codes de Welch peut être appliqué pour obtenir des codes de Golomb de longueur inférieure à (q-2). Si $\alpha + \beta = 1$ (α et β étant deux éléments primitifs de GF(q)), le premier élément de la matrice vaut 1; la première rangée et la première colonne peuvent alors être enlevées pour générer un code de Golomb de longueur (q-3) au lieu de (q-2).

Cette méthode permet de construire 12 codes différents de Golomb de longueur 128 à partir de GF(131). Les résultats obtenus pour la fonction d'auto-corrélation de ces codes sont semblables à ceux des autres codes de Golomb déjà étudiés. Le pic secondaire maximum se situe ici entre -13.8 dB et -17.7 dB par rapport au pic central pour un produit BT égal à la longueur du code(128) et au nombre d'éléments.

Les résultats obtenus pour l'auto-corrélation des codes de Golomb avec notre algorithme, sont présentés au tableau 3.

longueur	nombre d'éléments	minimum			maximum		
		α	β	pic [dB]	α	β	pic [dB]
125	125	7	55	-18.6	57	106	-12.9
126	9	tous	tous	- 8.9	--	---	------
128	128	17	115	-17.7	26	106	-13.8

Tableau 3 Auto-corrélation des codes de Golomb.

3. LES CODES À CONGRUENCES QUADRATIQUES

Les codes de Welch et de Golomb sont des codes de Costas car ils répondent au critère de Costas. Un type différent de construction de codes pour la modulation discrète de la fréquence, se base sur la théorie des congruences quadratiques; ce sont ce que nous appellerons les codes quadratiques. Contrairement aux codes de Costas, la séquence d'un code quadratique de longueur N n'est pas une permutation de l'ensemble {1,2,...,N}. Ces codes sont de type non-complet, certaines fréquences sont présentes plus d'une fois et d'autres ne sont jamais utilisées.

Une matrice représente les valeurs discrètes de la fréquence du code. La position de chaque élément (i,j) de la matrice représentant un code quadratique de longueur N est donnée par:

$$j = \left[\frac{a \cdot i \cdot (i-1)}{2} \right]_{\text{mod } N} \qquad (6)$$

$$1 \leq i \leq N$$
$$1 \leq a \leq N-1$$
$$a : \text{coefficient}$$

Avec cette méthode, on peut obtenir (N-1) codes différents de longueur N. Les matrices des codes quadratiques ont la propriété d'être symétriques par rapport à leur centre, c'est-à-dire que

$$(i,j) = (N+1-i,j) \quad \text{pour tout N impair}$$

Pour bien voir la symétrie des codes quadratiques, regardons à la figure 5 la matrice d'un code de longueur 9 ayant un coefficient égal à 5.

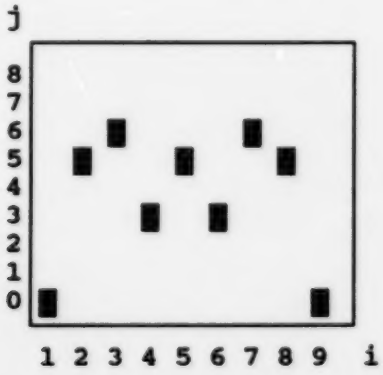


Figure 5 Code quadratique; N=9, a=5.

où les valeurs de i et j sont:

i	$j = 5 \cdot i \cdot (i-1)/2 \mid_{\text{mod } 9}$
1	$5 \cdot 1 \cdot 0/2 = 0 = 0$
2	$5 \cdot 2 \cdot 1/2 = 5 = 5$
3	$5 \cdot 3 \cdot 2/2 = 15 = 6$
4	$5 \cdot 4 \cdot 3/2 = 30 = 3$
5	$5 \cdot 5 \cdot 4/2 = 50 = 5$
6	$5 \cdot 6 \cdot 5/2 = 75 = 3$
7	$5 \cdot 7 \cdot 6/2 = 105 = 6$
8	$5 \cdot 8 \cdot 7/2 = 140 = 5$
9	$5 \cdot 9 \cdot 8/2 = 180 = 0$

Puisque la longueur du code doit être un nombre impair et premier, nous avons étudié les codes quadratiques de longueur 127. Les meilleurs résultats, c'est-à-dire les pics secondaires les plus faibles, ont été obtenus pour un coefficient de valeur égale à 15. Le pic secondaire principal est alors de -18.0 dB par rapport au pic central, et ceci pour un produit BT égal à la longueur du code ainsi qu'au nombre d'éléments, soit 127. Par contre, pour un coefficient de 107, le pic secondaire est à -15.8 dB par rapport au pic central. Pour toutes les autres valeurs du coefficient, entre 1 et 127, le niveau maximum des pics secondaires se situe entre ces deux bornes.

Dans l'article «Time-frequency hop signals part II: coding based upon quadratic congruences» [10] , l'auteur utilise aussi des nombres N impairs mais non premiers pour générer des codes quadratiques de longueur N. Étant donné la propriété qu'ont les codes quadratiques d'être symétriques par rapport à leur centre, nous générons un code de longueur 128 à partir d'un code de longueur 129 (impair, non premier) duquel nous retranchons l'élément central pour obtenir 128 éléments. Nous avons ensuite étudié les propriétés de ces codes quadratiques pairs. Lorsque le produit BT et le nombre d'éléments sont tous deux égaux à la longueur du code, ici 128, la valeur pointe des pics secondaires varie entre -0.4 dB et -14.2 dB sous le pic central.

Nous avons aussi étudié quelques autres cas de codes quadratiques pairs dont le nombre d'éléments est un facteur de la longueur du code. Nous obtenons pour un code quadratique de longueur et de produit BT 126 avec 18 éléments, des pics secondaires principaux entre -9.9 dB et -14.1 dB par rapport au pic central. Si le nombre d'éléments est égal à 14, les bornes des pics secondaires principaux sont -2.2 dB et -8.4 dB. Prenons des codes quadratiques de longueur et de produit BT de 128, avec successivement 8 et 16 éléments, on obtient respectivement des limites de -1.5 dB et -5.0 dB et de -9.8 dB à -13.8 dB pour les maximums des pics secondaires principaux.

Les codes quadratiques étudiés possèdent entre eux une fonction de corrélation croisée dont la valeur moyenne du maximum est à un niveau de -15.0 dB par rapport au pic central de leur fonction d'auto-corrélation. Les meilleurs résultats sont par contre obtenus avec les codes quadratiques pairs de longueur, produit BT et nombre d'éléments égaux à 128. La fonction de corrélation croisée pour ces codes est à -23.4 dB par rapport au pic principal de leur fonction d'auto-corrélation. Un exemple de fonction de corrélation croisée entre deux codes quadratiques pairs de longueur, produit BT et nombre d'éléments 128, possédant des coefficients de 41 et 86 est illustrée sur le graphique de la figure 6.

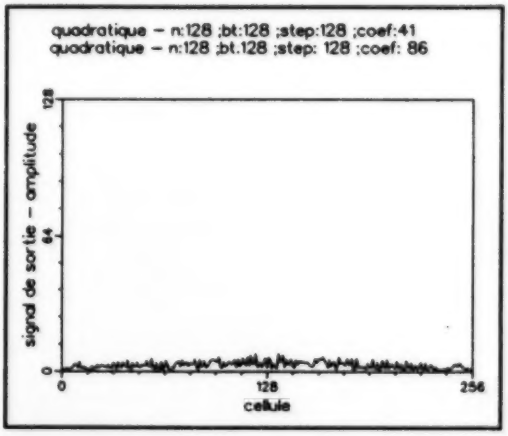


Figure 6 Corrélation croisée de codes quadratiques.

Le tableau 4 donne quelques résultats pour des codes possédant un produit BT égal à leur longueur. Les codes dont le nombre d'éléments est un facteur de la longueur du code n'offrent pas de meilleurs résultats ni au point de vue de la corrélation croisée, ni pour l'auto-corrélation.

longueur	nombre d' éléments	minimum η	minimum pic [dB]	maximum η	maximum pic [dB]
126	14	1	- 8.4	5	- 2.2
126	18	5	-14.1	15	- 9.9
126	126	13	-16.1	88	-12.5
127	127	15	-18.0	107	-15.6
128	8	2	- 5.0	6	- 1.5
128	16	2	-13.8	10	- 9.8
128	128	41	-14.2	86	- 0.4

Tableau 4 Auto-corrélation des codes quadratiques.

4. COMPARAISON DES DIFFÉRENTS TYPES DE CODES

Nous avons examiné les caractéristiques des trois différents types de codes. Les codes de Costas ont une fonction d'auto-corrélation offrant de meilleurs résultats que celle des codes quadratiques. Parmi les codes de Costas, les résultats obtenus montrent que les codes de Golomb offrent de moins bonnes possibilités que les codes de Welch pour la fonction d'auto-corrélation. Les meilleurs résultats obtenus par les codes de Golomb sont moins bons que n'importe quel résultat obtenu avec les codes de Welch lorsque le produit BT est égal à la longueur du code. Par exemple, pour des codes possédant une longueur, un produit BT et un nombre d'éléments égaux à 128, les résultats pour un code quadratique sont de -13.8 dB, de -17.7 dB pour un code de Golomb et de -21.5 dB pour un code de Welch.

En ce qui concerne la corrélation croisée, les résultats sont cependant semblables pour les deux types de codes de Costas, avec un maximum d'environ -13 dB à -14 dB par rapport à la valeur centrale de l'auto-corrélation qui est égale à la longueur du code. Les résultats obtenus pour la corrélation croisée des codes quadratiques est un peu meilleure avec une moyenne de -16 dB.

Les codes étudiés ci-haut sont aussi comparés avec d'autres types de codes qui ont déjà fait l'objet d'études, par exemple, les codes chirp, step-chirp et pseudo-aléatoires [12,11,1].

Nous avons comparé le code chirp de longueur et produit BT égaux à 100 et les codes step-chirp de même longueur et produit BT mais avec dix éléments avec les codes Welch et quadratiques de longueur et produit BT 100 ayant 10 ou 100 éléments. Les codes de Golomb ne sont pas testés puisque qu'ils n'existent pas pour les nombres d'éléments utilisés. Les résultats obtenus avec le code chirp sont meilleurs que les autres d'environ 3 dB à 12 dB. Les résultats obtenus avec le code step-chirp sont meilleurs que ceux des codes de Welch et quadratiques d'environ 6 dB à 15 dB.

Le code chirp de longueur et produit BT égales à 121 et le code step-chirp de même longueur et produit BT possédant 11 éléments ont été comparés aux codes de Golomb et quadratiques de mêmes longueur et produit BT ayant 11 éléments. Les codes de Welch n'existent pas dans ce cas. Le code chirp est, ici aussi, meilleur que les deux autres avec un pic secondaire maximum à -27.2 dB, ce qui est 5 dB de mieux que le code de Golomb et 15 dB de mieux que le code quadratique. Pour sa part, le code step-chirp offrent des résultats de 8 dB de mieux que les codes de Golomb et de 18 dB de mieux que les codes quadratiques avec un pic secondaire maximum de -30.7 dB.

Le tableau 5 montre les valeurs relatives des lobes secondaires de la fonction d'auto-corrélation pour les codes de Costas

(de Welch et de Golomb), quadratiques, chirp, step-chirp et pseudo-aléatoires. Ce tableau permet de comparer les résultats minimums et maximums obtenus avec des codes de longueur voisine de 128.

Code	Lobes secondaires	
	Minimum (longueur; éléments)	Maximum (longueur; éléments)
Welch	-24.0 dB (126; 126)	-13.8 dB (126; 18)
Golomb	-18.6 dB (125; 125)	-8.9 dB (126; 9)
Quadratique	-18.0 dB (127; 127)	-0.4 dB (128; 128)
Chirp	-27.4 dB (128; 128)	-26.3 dB (100; 100)
Step-Chirp	-30.7 dB (121; 11)	-29.8 dB (100; 10)
Pseudo-aléatoire	-24.0 dB (127; 127)	-18.0 dB (127; 127)

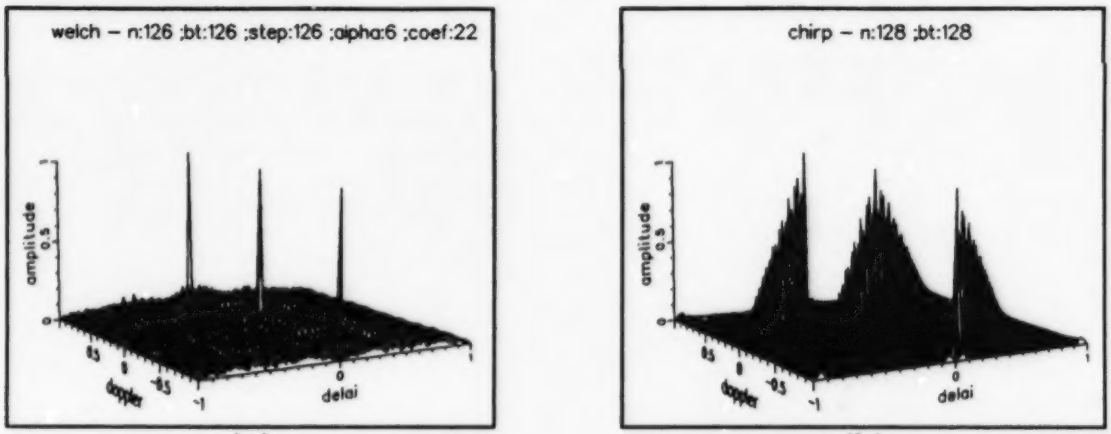
Tableau 5 Comparaison de l'auto-corrélation de différents codes.

Chaque code peut être caractérisé par un diagramme d'ambiguïté. Un diagramme d'ambiguïté est une représentation graphique de l'amplitude de la fonction d'ambiguïté, laquelle est la réponse de l'auto-corrélation pour différentes fréquences Doppler. Une cible possédant une vitesse radiale par rapport au radar se trouve à modifier la longueur d'onde du signal réfléchi. La fréquence Doppler est la différence entre la fréquence porteuse du signal transmis et celle du signal retourné, et peut être évaluée approximativement par :

$$f_d = 2 \cdot v_d / \lambda_o = 2 \cdot v_d \cdot f_o / c$$

Pour les diagrammes en forme de lame de couteau, comme ceux des codes chirp et step-chirp représentés à la figure 7b, il existe une ambiguïté entre la position réelle d'une cible en mouvement et celle donnée par le corrélateur. Pour les diagrammes en forme de punaise, comme ceux des codes binaires, des codes de Costas et des codes à congruences quadratiques représentés à la figure 7a, il

n'est pas possible de détecter une cible en mouvement dont la fréquence Doppler est supérieure à l'inverse de la longueur du code.



(a) (b)

Figure 7 a) Fonction d'ambiguïté d'un code de Costas.
b) Fonction d'ambiguïté d'un code chirp.

Les diagrammes d'ambiguïté des codes de modulation discrète de la fréquence peuvent être déterminés approximativement en superposant deux représentations graphiques de la matrice du code; une version demeure fixe tandis que l'autre est déplacée dans le plan fréquence/temps. L'amplitude de la fonction d'ambiguïté est alors proportionnelle au nombre d'éléments qui coïncident l'un sur l'autre. Une cible en mouvement crée un décalage de la fréquence initiale du signal sur l'axe des fréquences, occasionnant par le fait même un déplacement de la matrice sur l'axe des fréquences Doppler, tandis qu'un décalage en distance implique un déplacement de la matrice sur l'axe temporel.

La fréquence des codes chirp et step-chirp peut être représentée par une matrice avec une diagonale. Un déplacement de la matrice le long de la diagonale permet de coïncider presque tous les éléments des matrices et d'obtenir une bonne détection de la cible. L'amplitude de la fonction d'ambiguïté décroît proportionnellement avec ce déplacement, lequel nécessite en même temps un décalage en fréquence et un décalage temporel. Ces codes peuvent alors détecter, avec une ambiguïté en distance, des cibles en mouvement dont la fréquence Doppler est inférieure à la largeur de bande de la modulation B.

Les codes de Costas et quadratiques sont construits de façon à ce que la superposition d'une version décalée de la matrice sur une version fixe ne permet de coïncider que peu d'éléments. Ainsi, comme illustré à la figure 7a, le diagramme d'ambiguïté aura un pic principal à l'origine et de faibles lobes secondaires ailleurs dans le plan fréquence/temps. Pour cette raison ces codes permettent de

filtrer les cibles en mouvement dont la fréquence Doppler est supérieure à l'inverse de la longueur de l'impulsion transmise.

Pour qu'un code puisse être utilisé pour détecter une cible dont la vitesse est supérieure à la limite imposée par le diagramme d'ambiguïté, il est nécessaire de modifier les coefficients du filtre du compresseur de façon à déplacer le diagramme d'ambiguïté vers la fréquence Doppler correspondante. Une banque de plusieurs de ces filtres peuvent être utilisés parallèlement pour détecter une plus grande gamme de vitesses.

5. CONCLUSION

Ce rapport a permis d'étudier deux différents types de codages en fréquence, les codes de Costas et les codes à congruences quadratiques. Ces codes ont été évalués parce qu'ils permettent d'obtenir des diagrammes d'ambiguïté en forme de punaise tout en ayant de faibles lobes secondaires.

Les codes de Costas offrent de meilleurs résultats pour la fonction d'auto-corrélation du signal, surtout avec la méthode de construction de Welch. Ceux-ci sont en moyenne meilleurs de 5 dB par rapport aux codes de Golomb et de 10 dB par rapport aux codes quadratiques pour des longueurs voisine de 128. Les codes quadratiques ont par contre de plus faibles lobes pour la fonction de corrélation croisée. Ces codes permettent une probabilité réduite de détection du signal n'ayant pas le même code.

Les codes de Costas donnent de bons résultats pour la hauteur des lobes secondaires des fonctions d'auto-corrélation, mais pas aussi bien que d'autres codes déjà étudiés comme les codes chirp, step-chirp et pseudo-aléatoires. Quant aux codes quadratiques, ils pourraient être appropriés pour une utilisation nécessitant un compromis entre une bonne fonction d'auto-corrélation et une bonne corrélation croisée puisque les résultats de ces deux fonctions offrent alors d'assez bonnes possibilités.

BIBLIOGRAPHIE

[1] Blanchette, M., "La compression d'impulsion numérique appliquée au brouillage radar". Thèse de maîtrise, Université d'Ottawa, décembre 1991 (prévision).

[2] Painchaud, G.R. et M. Blanchette, "ECCM Advantages of Adaptive Digital Pulse Compression", Proceedings of the AGARD Avionics Panel Symposium on Electronic Counter-Counter Measures for Avionics Sensors and Communication Systems, pp. 16.1-16.6, octobre 1990.

[3] Blanchette, M., "L'utilisation de la compression d'impulsion numérique comme contre-contre-mesure électronique". DREO Signal Processing Workshop, mai 1991.

[4] Levanon, Nadav, "Radar Principles", John Wiley & Sons, New York, 1988, chap. 8.

[5] Costas, J.P., "A study of a class of detection waveforms having nearly ideal range-doppler ambiguity properties", Proceedings of the IEEE, vol. 72, no 8, août 1984, pp. 996-1009.

[6] Drumheller, D.M. et E.L. Titlebaum, "Cross-correlation properties of algebraically constructed Costas arrays", IEEE transactions on aerospace and electronic systems, vol. 27, no 1, janvier 1991, pp. 2-10.

[7] Golomb, S.W. et H. Taylor, "Constructions and properties of Costas arrays", Proceedings of the IEEE, vol. 72, no 9, septembre 1984, pp. 1143-1163.

[8] Bellegarda, J.R., "Congruential frequency hop signals for multi-user environments: a comparative analysis". Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, Albuquerque, NM, avril 1990, pp. 2903-2906.

[9] Titlebaum, E.L., S.V. Marić et J.R. Bellegarda, "Ambiguity properties of quadratic congruential coding". IEEE transactions on aerospace and electronic systems, vol. 27, no 1, janvier 1991, pp. 18-29.

[10] Sibul, L.H. et E.L. Titlebaum, "Time-frequency hop signals part II. Coding based upon quadratic congruences", IEEE transactions on aerospace and electronic systems, vol 17, no 4, juillet 1981, pp. 494-499.

[11] Lewis, B.L., F.F. Kretschmer, Jr. et W.W. Shelton, "Aspects of Radar Signal Processing", Artech House, Norwood, 1986, chap. 2.

[12] Painchaud, G.R., J.A.H. McKenzie, M. Blanchette et A. Voy, "An Experimental Adaptative Digital Pulse Compression Subsystem for Multi-Function Radar Applications", Proceedings of the IEEE International Radar Conference, pp. 153-158, mai 1990.

[13] Voy, A., "Final Report for the Digital Pulse Compression System Exploratory Development and Evaluation", Contract No. W7714-9-9110/01-ST, Compagnie Marconi Canada, Kanata, novembre 1990.

[14] Bastida, J.R., "Field extensions and Galois theory". New York: Cambridge University press, 1984, coll. Encyclopedia of mathematics and its applications, vol. 22. 294 p.

[15] Lin, S., "Error control coding: fundamentals and applications", New Jersey: Prentice Hall, 1983, coll. computer applications in electrical engineering, 603 p.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Centre de recherches pour la défense, Ottawa
Ottawa, Ontario, Canada K1A 0K2

2. SECURITY CLASSIFICATION (overall security classification of the document. including special warning terms if applicable)

Sans classification

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

L'application des codes de Costas et des codes à congruences quadratiques à la compression d'impulsion numérique. (U)

4. AUTHORS (Last name, first name, middle initial)

Delisle, Caroline
Blanchette, Martin

5. DATE OF PUBLICATION (month and year of publication of document)

Décembre 1991

6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)

28

6b. NO. OF REFS (total cited in document)

15

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

CRDO note technique

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

Centre de recherches pour la défense, Ottawa / Division du radar
Ottawa, Ontario, Canada K1A 0K2

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant)

Projet 041LC

9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)

CRDO note technique: n° 91-31

10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(X) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors; further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availabilty (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

Ministères de la Défense et entrepreneurs en matière de défense

SANS CLASSIFICATION

SECURITY CLASSIFICATION OF FORM

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both offical languages unless the text is bilingual).

Ce document étudie l'application à la compression d'impulsion numérique de deux types de codage de la fréquence: les codes de Costas et les codes à congruences quadratiques. Ces codes ont la particularité de produire des diagrammes d'ambiguité en forme de punaise avec de faibles lobes secondaires. Ce rapport traite des différents algorithmes de construction, de l'évaluation des fonctions d'auto-corrélation et de corrélation croisée, et de leur comparaison à des codes connus. Bien qu'ayant des résultats intéressants pour le nombre de codes disponibles et le niveau des lobes secondaires, ils semblent être moins performants sur ces points que les codes pseudo-aléatoires, "chirp" et "step-chirp".

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Radar

Compression d'impulsion numérique

Formes d'ondes codées

Codes de Costas

Codes à congruences quadratiques